ABSTRACT

A cryptosystem employing an identity-based ring signature by using bilinear pairings, which includes a user, a signer and a trusted authority, generates a set of system parameters shared by the user and the signer, generates a public key and a private key for the user and the signer by using the set of system parameters, thereby transmitting the generated public and the private keys to the user and the signer through a secure channel, respectively. The user conceals content of a message, requests a ring signature for the content-concealed message to the signer, and thereafter, verifies validity of the ID-based ring signature. The signer produces the ring signature based on identity (ID) of the user, thereby forming an ID-based ring signature for the content-concealed message.